Symmetry-based estimation of lower bound on secure key rate of noisy private states

Jan Tuziemski[1, 2] and Paweł Horodecki[1, 2]

[1]Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, PL-80-952 Gdańsk, Poland
[2]National Quantum Information Centre of Gdańsk, PL-81-824 Sopot, Poland

(Dated: February 5, 2013)

Quantum private states are the states that represent some amount of perfect secure key. A simple symmetry of any generalised private quantum state (ie. the states that represent perfect key but not fully random) is provided and extended on Devetak-Winter so called ccq (classical-classical-quantum) and cqq (classical-quantum-quantum) lower bound on secure key. This symmetry is used to develop a practical method of estimating the Alice measurement that is optimal form the perspective of single shot Devetak-Witner lower bound on secure key. The method is particularly good when the noise does not break the symmetry of the state with respect to the lower bound formula. It suggest a general paradigm for quick estimation of quantum communication rates under the symmetry of a given resource like state and/or channel.

I. INTRODUCTION

Entanglement is a considered as a resource in quantum communication and computing. It has many intriguing properties [1]. Any BB84 type protocol [2] is formally equivalent to some version of entangled based protocol of the type E91 [3]. Bennett et al. pointed out on specific scheme [4] which was later naturally extended to a quantum privacy amplification QPA [5] based entanglement distillation protocol [6]. The latter is a protocol that distills maximally entangled states out of a mixed states in a well defined way. In QPA it is eavesdropper that is representing the noise and the distillation procedure is aimed at remove the correlations with eavesdropper in the process that produces a pure output state - maximally entangled state that is a source of perfect key. It seemed that this QPA is necessary to get privacy. However there exists nondistillable entanglement called bound entanglement [7] for which by the very definition QPA in its original form can not work. It turns out that there is another possibility of distilling secret key by distilling private states [8] that are generalisations of maximally entangled states - they provide secret key under the measurement in a fixed basis on some part of the system. The measurement basis may be unique and that is what makes the private states more general form maximally entangled ones for which there are infinite many pairs of local bases that provide secure key. The distillation of private states allow to provide secret key form bound entanglement (see [8]) showing in particular a possibility of drastic separation between amount of pure entanglement that can be distilled from a quantum state (called distillable entanglement and denoted by D) and amount of secret key that can be distilled from the same state (called disiilalble secret key and denoted by K). Recently the separation $D < K$ was experimentally demonstrated together with the illustration how inefficient may be the original entanglement distillation based scheme, if compared with p-bit based protocols [9].

II. A USEFUL SYMMETRY OF THE GENERALISED PRIVATE STATES

According to [10] any state containing perfectly secure key corresponds to a pure state shared by three parties Alice, Bob and Eve. Unlike the eavesdropper subsystem E with a Hilbert space $\mathcal{H}_E$ the subsystems of Alice and Bob are composite and correspond to the tensor products of Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_{A'}$ and $\mathcal{H}_B \otimes \mathcal{H}_{B'}$ respectively. We call the subsystem corresponding to the pair A,B the key part since this is the part that is used for key generation by local von Neumann measurements while the pair A'B' is called the shield part since it is in a sense responsible for protecting the key. The above structure allows to write explicitly the pure state of the three parties which represents a perfectly secure random a perfectly secure random statistics $\vec{p} = [p_0, ..., p_{d-1}]$. It is a pure state $|\Psi_{AA'BB'}\rangle$ of the following form which we shall call *generalised private states*:

$$|\Psi_{AA'BB'E}\rangle = \sum_{ij} c_i c_j |ii\rangle_{AB} \otimes [U^{(i)}_{A'B'} \otimes I_E]|\Psi_{A'B'E}\rangle \tag{1}$$

for some fixed $|\Psi_{A'B'E}\rangle$, some unitaries $U^{(i)}_{A'B'}$ and probabilities $\{p_i = |c_i|^2\}$. The basis $|ii\rangle_{AB}$ is called the secure basis since after performing the local von Neumann measurements in that basis Alice and Bob share the correlated probability distribution $\{p^{ij}_{AB} = \delta_{ij} p_i\}_{i=0}^{d-1}$ which is completely uncorrelated form the system E. Here we do not assume them to be necessarily $p_i = \frac{1}{d}$ as it is in the case of the *private states*. In fact the density matrix corresponding to the

state vector (1) is of the form:

$$\rho_{priv} = \sum_{ij} c_i c_j [|ii\rangle\langle jj|]_{AB} \otimes [|\Psi_i\rangle\langle\Psi_j|]_{A'B'E}, \tag{2}$$

where we put $|\Psi_i\rangle = [U_{A'B'} \otimes I_E]|\Psi\rangle_{A'B'E}$ dropping the superscripts $A'B'E$. If Alice and Bob measure the subsystems AB in some basis $\{|e_i\rangle_A\}$, $\{|f_i\rangle_B\}$ and trace the shield subsystems $A'B'$ they get the so called *the form of the CCQ state with respect to the (product) basis* $\mathcal{B}_{AB} = \{|e_i f_i\rangle_{AB} \equiv |e_i\rangle_A \otimes |f_i\rangle_B\}$:

$$\rho_{ABE}^{CCQ,\mathcal{B}_{AB}}(\{|e_i, f_j\rangle\}) = \sum_{i=0}^{d-1} q_i \, |e_i\rangle\langle e_i|_A \otimes |f_i\rangle\langle f_i|_B \otimes \rho_E^i$$

with some probability distribution q_i. It happens that if they choose the basis $\{|e_i f_j\rangle_{AB}\}$ to be just equal to the secure one $\mathcal{B}_{AB}^0 = \{|ij\rangle_{AB}\}$ then the above state reduces to the product form

$$\rho_{ABE}^{CCQ,\mathcal{B}^0_{AB}} = (\sum_{i=0}^{d-1} p_i [|ii\rangle\langle ii|]_{AB}) \otimes \rho_E$$

with $q_i = p_i$. Because of the explicitly product form - no correlations of the E system with the key part AB are present here. Before proving some new property let us remind that the so called CQQ state with respect to the basis $\mathcal{B}_A = \{|e_i\rangle_A$ which results form Alice local von Neumann measurement and tracing out both A'B':

$$\rho_{ABE}^{CQQ,\mathcal{B}_A} = \sum_{i=0}^{d-1} q_i \, |e_i\rangle\langle e_i|_A \otimes \rho_{BE}^i \tag{3}$$

Note that measuring the private state in the local basis B_A^0 being just the reduction of the product secure basis $\mathcal{B}_{AB}^0$ we get still the CCQ state in the form (3) rather than the general CQQ state (note that any CCQ state is a CQQ one but not vice versa) which is a consequence of the private character of the state.

A. The Devetak-Winter protocol rates

We have a natural definition of the key rates in one-way protocols obtained by measuring the state first in some local basis $\mathcal{B}_A$ or a product one $\mathcal{B}_{AB}$ which will produce the CQQ or CCQ state respectively and then calculating the difference of the Holevo functions of the states:

$$K_{DW}^{\mathcal{B}_A}(\rho_{ABE}) = I_{A:B}(\rho_{AB}^{CQ}) - I_{A:E}(\rho_{AE}^{CQ}) \tag{4}$$

with ρ_{AB}^{CQ}, ρ_{AE}^{CQ} being a suitable reductions of the state $\rho_{ABE}^{CQQ,\mathcal{B}_A}$ resulting form the original state ρ_{ABE} after the local Alice measurement associated with the basis $\mathcal{B}_A$. In full analogy we have

$$K_{DW}^{\mathcal{B}_{AB}}(\rho_{ABE}) = I_{A:B}(\rho_{AB}^{CC}) - I_{A:E}(\rho_{AE}^{CQ}) \tag{5}$$

with the suitable reductions of the state $\rho_{ABE}^{CCQ,\mathcal{B}_{AB}}$ resulting form the original state ρ_{ABE} after the product of the two local Alice and Bob measurements corresponding to the bases $\mathcal{B}_{AB}$. The role of the function f is played just by the mutual information function I.

B. General symmetry rule and its simple application

In what follows we shall use the notation $\hat{U}(X) = UXU^\dagger$ and $\hat{M}(\{P_k\})(X) = \sum_k P_k X P_k$ with a projectors $P_k = P(e_k) = |e_k\rangle\langle e_k|$ for any orthonormal basis $\{e_k\}$. We have a simple

Observation .- Consider a function f defined on any CQ state on the composite system XY

$$\sigma_{XY}^{CQ} = \sum_k P_k \otimes \sigma_k \tag{6}$$

Assume that the function f is invariant under some subgroup $\mathcal{R}_X$ of unitary operations $R_X \in \mathcal{R}_X$ on the system X ie.

$$\forall_{R_X \in \mathcal{R}_X} f(\hat{R}_X \otimes \hat{I}_Y(\sigma_{XY}^{CQ}) = f(\sigma_{XY}^{CQ}) \tag{7}$$

Given any state ρ_{XY} which is invariant in an analogous way

$$\forall_{R_X \in \mathcal{R}_X} \hat{R}_X \otimes \hat{I}_Y(\rho_{XY}) = \rho_{XY} \tag{8}$$

we have the following identity

$$f([\hat{M}_X(\{\hat{R}_X(P_k)\}) \otimes \hat{I}_Y](\rho_{XY})) = f([\hat{M}_X(\{P_k\}) \otimes \hat{I}_Y](\rho_{XY})) \tag{9}$$

for all $R_X \in \mathcal{R}_X$ and all $\{P_k\}$ constructed from any orthonormal bases $\{e_k\}$.

Proof. - It is obvious to see that „internal" $\hat{R}_X^{\dagger}$ is absorbed by the QQ state ρ_{XY} while the external conjugated one $\hat{R}_X$ is absorbed by the invariance of the function f.

We have immediate conclusion:

Conclusion.- The functions (4) and (5), if calculated on a given generalised private state (2), are invariant under the rotations $\hat{R}_A \otimes \hat{I}_{BE}$ and $\hat{R}_A \otimes \hat{R}_B \otimes \hat{I}_E$ respectively where R_A, R_B are any unitary operations which are diagonal in the local bases $|i\rangle_A$, $|j\rangle_B$ forming a secure basis of the states (2).

Proof .- The role of the pair of the subsystems $\{X, Y\}$ is played by $\{A, BE\}$ or $\{AB, E\}$ respectively and the role of the subgroup are all the unitary operations diagonal in the bases described in the conclusion.

C. Consequences

In the case, when the key part dimension $d = 2$, this feature can be interpreted graphically. Let us consider CQQ case. Then Alice can choose two angels (θ, φ) to determine her measurement basis using the eigenvectors of the $\sigma_{\hat{n}}$ operator

$$|e_0(\theta,\varphi)\rangle = \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{\mathrm{i}\varphi}\sin\frac{\theta}{2} \end{bmatrix}, |e_1(\theta,\varphi)\rangle = \begin{bmatrix} \sin\frac{\theta}{2} \\ -e^{\mathrm{i}\varphi}\cos\frac{\theta}{2} \end{bmatrix}. \tag{10}$$

We define the function $K_D(\theta,\varphi) = K_D^{DW}\left(\rho_{priv}^{C(\theta,\varphi)QQ}\right)$. Here superscript $C(\theta, \varphi)$ denotes that to calculate CQQ state base vectors determined by angels (θ, φ) were used. In spherical coordinate system, in which $|e_0(0,0)\rangle, |e_1(0,0)\rangle$ coincide with the base vectors used in (2) the function $K_D(\theta,\varphi)$ is φ independent, i.e. becomes function only of θ angle.

III. PROCEDURE

As follows from the previous section, points on the sphere[1] possessing the same vale of K_D establish a circle, whose center is located at intersection of Z axis and the sphere. Moreover, each circle has a center in the same point (all circles are concentric). At this point vale of K_D is maximal. Using facts presented in Subsection II C one is able to find such angles θ_{Max}, φ_{Max}, for which the measurement in basis given by (10) will lead to the maximal value of K_D, without a priori knowledge of this basis or rotations by which the state was changed. Suppose that the original ideal state was rotated by unknown transformation $U_A \otimes I_{BA'B'}$ which eventually changed its optimal measurement basis on Alice side from $\{|0_{\hat{z}}\rangle, |1_{\hat{z}}\rangle\}$ to $\{|0_{\hat{n}}\rangle, |1_{\hat{n}}\rangle\}$ where we define $\hat{n} = O\hat{z}$ as:

$$\begin{aligned} |0_{\hat{n}}\rangle\langle 0_{\hat{n}}| &= U|0_{\hat{z}}\rangle\langle 0_{\hat{z}}|U^{\dagger} = \frac{1}{2}(I + (O\hat{z})\vec{\sigma}) \\ |1_{\hat{n}}\rangle\langle 1_{\hat{n}}| &= U|1_{\hat{z}}\rangle\langle 1_{\hat{z}}|U^{\dagger} = \frac{1}{2}(I - (O\hat{z})\vec{\sigma}). \end{aligned} \tag{11}$$

The procedure is as follows.

[1] Points on the sphere correspond to angles used in (10). The term sphere should not be confused with the Bloch sphere of the state.

1. First one chooses arbitrary values of angles θ_0, φ_0 and establishes two base vectors $|e_0(\theta_0, \varphi_0)\rangle$ and $|e_1(\theta_0, \varphi_0)\rangle$. This basis is used to perform measurement and to obtain value of $K_D(\theta_0,\varphi_0)$ equal K_{D0}.

2. Then one changes the value of θ_0 to θ_1 and creates a set of base vectors $\{|e_0(\theta_1, \varphi_i)\rangle, |e_1(\theta_1, \varphi_i)\rangle\}_{i=1}^{N}$. Vectors from this set differ in the value of φ_i angle by arbitrary constant factor $\frac{2\pi}{N}$ so that $0 \leq \varphi_i < 2\pi$. One can ascribe each vector from the set to a corresponding point on the sphere. These points lay on a circle, whose centre is located at the point ascribed to vector $|e_0(\theta_0, \varphi_0)\rangle$.

3. Subsequently, using the vectors from the set, the measurements are performed and for each pair of vectors $|e_0(\theta_1, \varphi_i)\rangle, |e_1(\theta_1, \varphi_i)\rangle$ the value of K_{Di} is calculated. A set of values $K_{D,N} = \{K_{D1}, \ldots, K_{DN}\}$ is created. The aim of these measurements is to find two points laying on a chosen circle, characterized by values of φ_i angle, for which value of K_{Di} is equal to earlier calculated value K_{D0}. It is not difficult to see that it is always possible to achieve this purpose when we assume continuity of φ (or arbitrary small resolution in φ_i). According Subsection II C, because the sphere is covered with circles with the same value of K_D, any other circle laying on the sphere can have 0, 1, 2 or infinity intersection points. Thus it is always possible to find such values of θ_0, θ_1, which ensure that points with the same value of K_D are found. Just as for a plane, three points on the sphere are enough to unambiguously determine the circle. The radius and the centre of the circle are found solving the system of equations:

$$d(\theta_{Max}, \varphi_{Max}, \theta_0, \varphi_0) = R \tag{12}$$
$$d(\theta_{Max}, \varphi_{Max}, \theta_1, \varphi_1) = R \tag{13}$$
$$d(\theta_{Max}, \varphi_{Max}, \theta_1, \varphi_2) = R, \tag{14}$$

where d is spherical distance defined as [12]:

$$d = \arccos(\mathbf{P} \cdot \mathbf{Q}), \tag{15}$$

here $\mathbf{P}$, $\mathbf{Q}$ are two points on the sphere characterized by angles θ_i, φ_i and θ_j, φ_j, respectively. In therms of Cartesian coordinates ($x = \sin\theta\cos\varphi$, $y = \sin\theta\sin\varphi$ and $z = \cos\theta$) expression (15) is of a form:

$$\begin{aligned} &d(\theta_i, \varphi_i, \theta_j, \varphi_j) = \\ &= \arccos(\sin\theta_i \sin\theta_j \cos(\varphi_i - \varphi_j) + \cos\theta_i \cos\theta_j). \end{aligned} \tag{16}$$

According to Subsection II C centre of the circle determined in this way is associated with the basis (characterized by angles θ_{Max}, φ_{Max}), in which $K_D(\theta, \varphi)$ has maximal value. Fig. 1 presents main ideas of the proposed procedure.

The proposed procedure can be slightly modified. Finding two points with value of K_{Di} exactly equal K_{D0} can cause a problem and such solution is not a practical one. To overcome this difficulty, instead of finding two points with the same value of K_D, one finds points K_{D1}, K_{D2} from the set $K_{D,N}$, for which the values of K_{D1}, K_{D2} are the closest to the K_{D0} i.e. for which $\Delta K_{D1} = K_{D0} - K_{D1}$ and $\Delta K_{D2} = K_{D0} - K_{D2}$ are minimal. Subsequently the interpolating function $I_{\{K_{D,N}\}}(\theta_1, \varphi)$ from the set $K_{D,N}$ is created. To construct the interpolation function Hermite polynomials of a required order are used. Thus one can write for $i = \{1, 2\}$:

$$\begin{aligned} K_{D0} &= \\ &= K_{Di} + \Delta K_{Di} = \\ &= K_D(\theta_1, \varphi_i) + \left.\frac{\partial I_{\{K_{D,N}\}}(\theta_1, \varphi)}{\partial\varphi}\right|_{\varphi=\varphi_i} \Delta\varphi_i \\ &\quad + \left.\frac{\partial^2 I_{\{K_{D,N}\}}(\theta_1, \varphi)}{\partial\varphi^2}\right|_{\varphi=\varphi_i} \Delta\varphi_i^2 = \\ &= I_{\{K_{D,N}\}}(\theta_1, \varphi_i) + \left.\frac{\partial I_{\{K_{D,N}\}}(\theta_1, \varphi)}{\partial\varphi}\right|_{\varphi=\varphi_i} \Delta\varphi_i \\ &\quad + \left.\frac{\partial^2 I_{\{K_{D,N}\}}(\theta_1, \varphi)}{\partial\varphi^2}\right|_{\varphi=\varphi_i} \Delta\varphi_i^2, \end{aligned} \tag{17}$$

where we use the fact that $I_{\{K_{D,N}\}}(\theta_1, \varphi_i) = K_{Di}$ (i.e. the interpolation function reproduces the values of K_{Di} from the set $K_{D,N}$ in the probe points). One solves equation (17) for $\Delta\varphi_i$, $i = \{1, 2\}$. In general, equation (17) can have

two different solutions. However, in such a case one chooses smaller $\Delta\varphi_1$ and $\Delta\varphi_2$ (because equation (17) is Taylor expansion of function $I_{\{K_{D,N}\}}(\theta_1,\varphi)$ near $\varphi=\varphi_i$). By solving modified systems of equations:

$$d(\theta_{Max},\varphi_{Max},\theta_0,\varphi_0)=R \tag{18}$$
$$d(\theta_{Max},\varphi_{Max},\theta_1,\varphi_1+\Delta\varphi_1)=R \tag{19}$$
$$d(\theta_{Max},\varphi_{Max},\theta_1,\varphi_2+\Delta\varphi_2)=R, \tag{20}$$

one obtains values of $\theta_{Max},\varphi_{Max}$.
The proposed approach enables to find the basis optimizing the value of K_D by performing only local measurements.

IV. ERROR ESTIMATION

Due to approximation (finite sum) and possible numerical errors, it is never possible to solve (17) exactly. As a result angles θ'_M,φ'_M will not lead to the maximal value of distillable key. In this section the estimation of this error is provided. Let us denote (see Fig. 2):

$$\begin{aligned}
\tilde{\varphi}_1 &= \varphi_1+\Delta\varphi_1=\varphi'_1+\Delta\varphi'_1\\
\tilde{\varphi}_2 &= \varphi_2+\Delta\varphi_2=\varphi'_2+\Delta\varphi'_2\\
\theta_M+\Delta\theta_M &= \theta'_M\\
\varphi_M+\Delta\varphi_M &= \varphi'_M.
\end{aligned} \tag{21}$$

Without loss of generality, we can arrange $\tilde{\varphi}_1,\tilde{\varphi}_2$ so that $\tilde{\varphi}_1>\tilde{\varphi}_2$. Spherical distance between points characterized by angles (θ_i,φ_i), (θ_j,φ_j) is given by (15). We assume that $(\theta_i,\varphi_i)=(0,0)$, so

$$\arccos\left[\cos\theta'_M\right]=R \tag{22}$$
$$\arccos\left[\sin\theta_1\sin\theta'_M\cos\left(\tilde{\varphi}_1-\varphi'_M\right)+\cos\theta_1\cos\theta'_M\right]=R \tag{23}$$
$$\arccos\left[\sin\theta_1\sin\theta'_M\cos\left(\tilde{\varphi}_2-\varphi'_M\right)+\cos\theta_1\cos\theta'_M\right]=R. \tag{24}$$

Combining 23 and 24 we get:

$$\cos\left(\tilde{\varphi}_1-\varphi'_M\right)=\cos\left(\tilde{\varphi}_2-\varphi'_M\right). \tag{25}$$

Because $\tilde{\varphi}_1\neq\tilde{\varphi}_2$ and $\varphi'_M\in(0,2\pi]$ there are two possibilities: $\tilde{\varphi}_1-\varphi'_M=-\left(\tilde{\varphi}_2-\varphi'_M\right)$ or $\tilde{\varphi}_1-\varphi'_M=-\left(\tilde{\varphi}_2-\varphi'_M-2\pi\right)$. We set $\varphi'_M:=\varphi'_M\ mod\ 2\pi$

$$\begin{aligned}
\varphi'_M &= \frac{\tilde{\varphi}_1+\tilde{\varphi}_2}{2}\\
\varphi_M+\Delta\varphi_M &= \frac{\varphi_1+\varphi_2}{2}+\frac{\Delta\varphi_1+\Delta\varphi_2}{2},
\end{aligned} \tag{26}$$

so $\Delta\varphi_M=\frac{\Delta\varphi_1+\Delta\varphi_2}{2}$. However, we know only $\varphi'_i,\ \Delta\varphi'_i$ but we can estimate (see Fig. 2) as $|\Delta\varphi_i|<\Delta\varphi-|\Delta\varphi'_i|$. As a result

$$\Delta\varphi_M<\frac{2\Delta\varphi-|\Delta\varphi'_1|-|\Delta\varphi'_2|}{2}. \tag{27}$$

Combining equations (22) and (23)

$$\cot\theta'_M=\cot\frac{\theta_1}{2}\cos\left(\tilde{\varphi}_1-\varphi'_M\right). \tag{28}$$

As a consequence of the equality

$$\begin{aligned}
&\cos\left(\tilde{\varphi}_1-\varphi'_M\right)=\cos\left(\varphi_1+\Delta\varphi_1-\frac{\varphi_1+\Delta\varphi_1+\varphi_2+\Delta\varphi_2}{2}\right)=\\
&\cos\left(\frac{\varphi_1+\Delta\varphi_1-\varphi_2-\Delta\varphi_2}{2}\right),
\end{aligned} \tag{29}$$

we obtain the following relation

$$\theta_M = \operatorname{arccot}\left[\cot\frac{\theta_1}{2}\cos\left(\frac{\varphi_1-\varphi_2}{2}\right)\right] \tag{30}$$

and

$$\theta_M + \Delta\theta'_M = \operatorname{arccot}\left[\cot\frac{\theta_1}{2}\cos\left(\tilde{\varphi}_1-\varphi'_M\right)\right]. \tag{31}$$

In order to obtain the upper bound on $\Delta\theta'_M$ we have to find $\bar{\theta}_M$ - an lower bound on θ_M. Then the following relation holds:

$$\bar{\theta}_M + \Delta\theta'_M < \theta_M + \Delta\theta'_M = \operatorname{arccot}\left[\cot\frac{\theta_1}{2}\cos\left(\tilde{\varphi}_1-\varphi'_M\right)\right], \tag{32}$$

so $\Delta\theta'_M < \operatorname{arccot}\left[\cot\frac{\theta_1}{2}\cos\left(\tilde{\varphi}_1-\varphi'_M\right)\right] - \bar{\theta}_M$. We have to estimate the difference $\varphi_1-\varphi_2$ using known quantities $\tilde{\varphi}_1, \tilde{\varphi}_2$. There are two different possibilities: in the first one $\tilde{\varphi}_1-\tilde{\varphi}_2 < \pi$ whereas in the second $\tilde{\varphi}_1-\tilde{\varphi}_2 > \pi$. Let us consider the first one. Because $\operatorname{arccot} x \in (-\frac{\pi}{2}, \frac{\pi}{2}]$ is a decreasing function for $x \in (-\infty, 0) \cup (0, \infty)$, in order to find $\bar{\theta}_M$ we have to increase $\cos\left(\frac{\varphi_1-\varphi_2}{2}\right)$. For our purposes we shall assume the worst case, namely $\tilde{\varphi}_1 < \varphi_1$ and $\tilde{\varphi}_2 > \varphi_2$. Then $\varphi_1-\varphi_2 > \tilde{\varphi}_1-\tilde{\varphi}_2$. From previous considerations the following relation holds: $\tilde{\varphi}_i + \Delta\varphi > \varphi_i > \tilde{\varphi}_i - \Delta\varphi_i$. As a result $\tilde{\varphi}_1-\tilde{\varphi}_2+2\Delta\varphi > \varphi_1-\varphi_2 > \tilde{\varphi}_1-\tilde{\varphi}_2$. Using this inequality we get

$$\theta_M > \bar{\theta}_{M1} = \operatorname{arccot}\left[\cot\frac{\theta_1}{2}\cos\left(\frac{\tilde{\varphi}_1-\tilde{\varphi}_2+2\Delta\varphi}{2}\right)\right]. \tag{33}$$

If $\tilde{\varphi}_1-\tilde{\varphi}_2 > \pi$ the similar line of reasoning leads to

$$\theta_M > \bar{\theta}_{M2} = \operatorname{arccot}\left[\cot\frac{\theta_1}{2}\cos\left(\frac{\tilde{\varphi}_1-\tilde{\varphi}_2-2\Delta\varphi}{2}\right)\right]. \tag{34}$$

Finally one gets

$$\Delta\theta'_M < \operatorname{arccot}\left[\cot\frac{\theta_1}{2}\cos\left(\tilde{\varphi}_1-\varphi'_M\right)\right] - \bar{\theta}_{Mi}, \tag{35}$$

where $\bar{\theta}_{Mi}, i=\{1,2\}$ is given by (33) or (34). Using perturbed points $(\theta_i, \tilde{\varphi}_i)$ one obtains the point $(\theta_M+\Delta\theta_M, \varphi_M+\Delta\varphi_M)$which differs from the real point (θ_M, φ_M) by $(\Delta\theta_M, \Delta\varphi_M)$, where $\Delta\theta_M, \Delta\varphi_M$ are given by (31) and (27). In the new coordinate system associated with the point $(\theta_M+\Delta\theta_M, \varphi_M+\Delta\varphi_M)$ the error is given by:

$$\begin{aligned}\Delta\theta = \arccos[\quad & \sin\theta'_M \sin\left(\theta'_M-\Delta\theta_M\right)\cos\Delta\phi_M \;+ \\ & +\cos\theta'_M\cos\left(\theta'_M-\Delta\theta_M\right)].\end{aligned} \tag{36}$$

V. INVARIANCE AND CHANNELS

According to [10], using appropriate unitary operation $U = 1_A \otimes \sum_i |i\rangle\langle i| \otimes U^{(i)}_{A'B'}$ (called twisting) it is possible to write a particular private state as:

$$\rho_{priv} = |\Psi_+\rangle\langle\Psi_+|_{AB} \otimes \sigma_{A'B'}, \tag{37}$$

where $|\Psi_+\rangle$ is one of the four Bell states $|\Psi_\pm\rangle$, $|\phi_\pm\rangle$

$$|\Psi_\pm\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \quad |\phi_\pm\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}. \tag{38}$$

After sending (37) down the channel $\Lambda_A \otimes I$ where $\Lambda_A(\cdot) = \sum_i p_i K_i(\cdot)K_i^\dagger$ with $K_i = \{I, \sigma_x, \sigma_y, \sigma_z\}$ one obtains a state

$$\begin{aligned}\tilde{\rho}_{priv} =& p_1|\Psi_+\rangle\langle\Psi_+|_{AB} \otimes \sigma_{A'B'} + p_4|\Psi_-\rangle\langle\Psi_-|_{AB} \otimes \sigma_{A'B'} \\ & p_2|\phi_+\rangle\langle\phi_+|_{AB} \otimes \sigma_{A'B'} + p_3|\phi_-\rangle\langle\phi_-|_{AB} \otimes \sigma_{A'B'}.\end{aligned} \tag{39}$$

The purification of this state is given by

$$
\begin{aligned}
\left|\tilde{\Psi}\right\rangle_{priv} =& \frac{p_1}{\sqrt{2}} \left(|00\rangle_{AB} \left|\Psi^0_\sigma\right\rangle_{ABE} + |11\rangle_{AB} \left|\Psi^1_\sigma\right\rangle_{ABE} \right) |0\rangle_{\bar{E}} \\
& \frac{p_4}{\sqrt{2}} \left(|00\rangle_{AB} \left|\Psi^0_\sigma\right\rangle_{ABE} - |11\rangle_{AB} \left|\Psi^1_\sigma\right\rangle_{ABE} \right) |1\rangle_{\bar{E}} \\
& \frac{p_2}{\sqrt{2}} \left(|01\rangle_{AB} \left|\Psi^0_\sigma\right\rangle_{ABE} + |10\rangle_{AB} \left|\Psi^1_\sigma\right\rangle_{ABE} \right) |2\rangle_{\bar{E}} \\
& \frac{p_3}{\sqrt{2}} \left(|01\rangle_{AB} \left|\Psi^0_\sigma\right\rangle_{ABE} - |10\rangle_{AB} \left|\Psi^1_\sigma\right\rangle_{ABE} \right) |3\rangle_{\bar{E}} ,
\end{aligned}
\tag{40}
$$

where $\bar{E}$ denotes new Eves' subsystem. We calculate the cqq state using base vectors defined by (10). The nonzero elements of the reduced AB matrix are given by

$$
\begin{aligned}
& a_{0000} = e_{00} \left[\cos^2 \frac{\theta}{2} (p_1 + p_4) + \sin^2 \frac{\theta}{2} (p_2 + p_3) \right] \\
& a_{0101} = e_{11} \left[\sin^2 \frac{\theta}{2} (p_1 + p_4) + \cos^2 \frac{\theta}{2} (p_2 + p_3) \right] \\
& a_{1010} = e_{00} \left[\sin^2 \frac{\theta}{2} (p_1 + p_4) + \cos^2 \frac{\theta}{2} (p_2 + p_3) \right] \\
& a_{1111} = e_{11} \left[\cos^2 \frac{\theta}{2} (p_1 + p_4) + \sin^2 \frac{\theta}{2} (p_2 + p_3) \right] \\
& a_{0010} = a^*_{0100} = e_{01} \left[e^{i\varphi} \sin \frac{\theta}{2} \cos \frac{\theta}{2} (p_1 - p_4) + \right. \\
& \left. e^{-i\varphi} \sin \frac{\theta}{2} \cos \frac{\theta}{2} (p_2 - p_3) \right] \\
& a_{1011} = a^*_{1110} = e_{01} \left[e^{i\varphi} \sin \frac{\theta}{2} \cos \frac{\theta}{2} (p_4 - p_1) + \right. \\
& \left. e^{-i\varphi} \sin \frac{\theta}{2} \cos \frac{\theta}{2} (p_3 - p_2) \right] .
\end{aligned}
\tag{41}
$$

The reduced AB matrix is block diagonal so its eigenvalues are

$$
\begin{aligned}
\lambda_1 &= \frac{1}{2} \left(a_{0000} + a_{0101} \pm \sqrt{(a_{0000} + a_{0101})^2 - 4 |a_{0001}|^2} \right) \\
\lambda_2 &= \frac{1}{2} \left(a_{1010} + a_{1111} \pm \sqrt{(a_{1010} + a_{1111})^2 - 4 |a_{0111}|^2} \right) .
\end{aligned}
\tag{42}
$$

As a consequence, $I_{(A:B)}$ will be independent of φ angle if and only if $(p_1 - p_4) = 0$ or $(p_2 - p_3) = 0$. Moreover $I_{(A:B)}(\theta) \leq I_{(A:B)}(0)$. To show that $I_{(A:E\bar{E})}(\theta, \varphi) \geq I_{(A:E\bar{E})}(0, \varphi)$ let us consider a state resulting from the measurement performed on $\bar{E}$ subsystem. This operation does not increase the value of $I_{(A:E\bar{E})}$. Then, the reduced AE$\bar{E}$ matrix resulting from the measurement has following eigenvalues $\lambda_{1,2} = \frac{p_1}{2}, \lambda_{1,2} = \frac{p_2}{2}, \lambda_{1,2} = \frac{p_3}{2}, \lambda_{1,2} = \frac{p_4}{2}$, so we obtain $I_{(A:E)}(\theta, \varphi) = I_{(A:E)}(0, \varphi)$.

VI. NUMERICAL RESULTS

In this section we provide some examples of the results obtained by implementing the above procedure numerically. *Rotated* ρ_{SWAP} *state.* - Consider a private state introduced in [8] and realized experimentally [11]

$$
\begin{aligned}
\rho_{SWAP} = \quad & \frac{1}{4} |\Psi_-\rangle \langle \Psi_-|_{AB} \otimes |\Psi_-\rangle \langle \Psi_-|_{A'B'} + \\
& \frac{1}{4} |\Psi_+\rangle \langle \Psi_+|_{AB} \otimes I_{A'B'} \\
& -\frac{1}{4} |\Psi_+\rangle \langle \Psi_+|_{AB} \otimes |\phi_-\rangle \langle \phi_-|_{A'B'} .
\end{aligned}
\tag{43}
$$

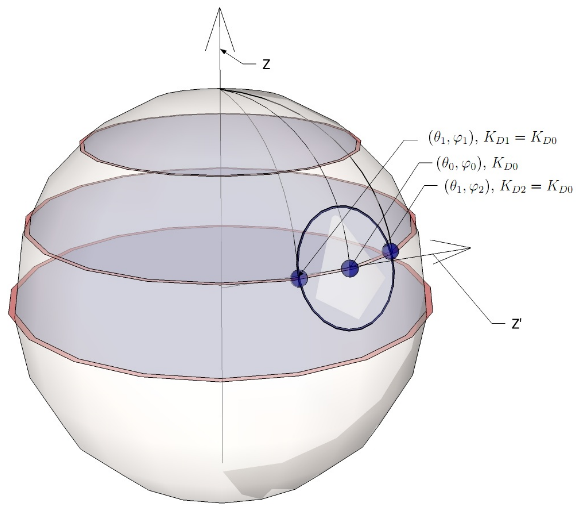

FIG. 1: Local Alice's sphere with two different coordinate systems. Z axis corresponds to θ_{Max}, φ_{Max} angles whereas Z' to θ_0, φ_0 angles. Black circle shows the path along which angle φ changes. At the intersection point between Z axis and the sphere $K_D(\theta_{Max}, \varphi_{Max}) = K_{DMax}$. The intersection point between Z' axis and the sphere is denoted by (θ_0, φ_0). At this point $K_D(\theta_0, \varphi_0) = K_{D0}$. Points with the same value of K_D (laying on a circle, whose center is located at the point K_{D0}) are denoted by (θ_1, φ_1) and (θ_1, φ_2). At the first point $K_D(\theta_1, \varphi_1) = K_{D1}$, whereas at the second point $K_D(\theta_1, \varphi_2) = K_{D2}$.

This state was rotated and then the optimizing procedure was applied. The example of the results is shown in Fig. 3.

Depolaraizig channel. - The procedure was checked using the rotated state $\rho_{S\tilde{W}AP} = \Lambda_A \otimes I_{BA'B'}$, where $\Lambda(\rho) = p\frac{I}{2} + (1-p)\rho$. The example of the results is shown in Fig. 4.

Phase flip channel. - Another test was performed using the rotated $\rho_{S\tilde{W}AP} = \Lambda_A \otimes I_{BA'B'}$, where $\Lambda(\rho) = p\rho + (1-p)\sigma_z\rho\sigma_z$. The example of the results is shown in Fig. 5.

Rotated mixture of ρ_{SWAP} and ρ_{MSWAP} states. - Another example of the private states is a state

$$\begin{aligned}\rho_{MSWAP} = \quad & \frac{1}{2}\left|\phi_-\right\rangle\left\langle\phi_-\right| \otimes \left(\frac{1}{2}\left|00\right\rangle\left\langle 00\right| + \left|\Psi_+\right\rangle\left\langle\Psi_+\right|\right) + \\ & +\frac{1}{2}\left|\phi_+\right\rangle\left\langle\phi_+\right| \otimes \left(\frac{1}{2}\left|11\right\rangle\left\langle 11\right|\left|\Psi_-\right\rangle\left\langle\Psi_-\right|\right). \end{aligned} \tag{44}$$

This state plays a role in bound entangled secure key [13]. We checked the procedure using rotated mixture of two private states $\rho_{priv} = p\rho_{SWAP} + (1-p)\rho_{MSWAP}$ and the rotated $\rho_{S\tilde{W}AP} = \Lambda_A \otimes I_{BA'B'}$, where $\Lambda(\rho) = p\rho + (1-p)\sigma_z\rho\sigma_z$. The example of the results is shown in Fig. 6.

Qubit channel with trigonometrical parametrization. - Consider a channel given by the Kraus operators [14]

$$\begin{aligned} K_1 &= \left[\cos\frac{u}{2}\cos\frac{v}{2}\right] I + \left[\sin\frac{u}{2}\sin\frac{v}{2}\right]\sigma_z \\ K_2 &= \left[\cos\frac{u}{2}\sin\frac{v}{2}\right]\sigma_x - \mathrm{i}\left[\sin\frac{u}{2}\cos\frac{v}{2}\right]\sigma_y \end{aligned} \tag{45}$$

which transforms the Bloch vector $\vec{r} = [r_x, r_y, r_z]^T$ of the state into $\vec{r'} = [\cos u r_x, \cos v r_y, \cos u \cos v r_z + \sin u \sin v]^T$. It follows from Section V that in general this channel does not preserve the invariance of distillable key. In this case the procedure fails. The example of the results is shown in Fig. 7.

VII. CONCLUSIONS

In the present paper the new symmetry of the states with perfect secure key called generalized private states have been provided which says that the most popular Devetak-Winter secret key rate is invariant in both scenarios of CCQ and CQQ type if the measurement bases, chosen in a wrong way, are rotated (in a sense of angular momentum) in addition around the axis corresponding to the secure basis by any angle. The symmetry has a particularly good interpretation when seen on a sphere since then the wrong is any basis corresponding to $\hat{n}$ with an angle θ to the $\hat{z}$ axis (corresponding to the secure basis) while the symmetry rotation is just the rotation by the ϕ angle around the

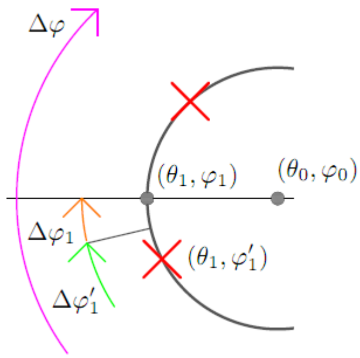

FIG. 2: Starting point for the procedure (θ_0, φ_0), in which $K(\theta_0, \varphi_0) = K_{D0}$. Point (θ_1, φ_1'), $K_{D0} = K(\theta_1, \varphi_1')$ is closest to the point (θ_0, φ_0) in the given set because$\Delta K_{D1} = |K_{D0} - K_{D1}|$ is minimal (see text for details). Using the interpolation function one obtains that $K(\theta_1, \varphi_1' + \Delta\varphi_1') = K_{D0}$, however, due to numerical error, in fact $\varphi_1' + \Delta\varphi_1' \neq \varphi_1$, where the equality $K_D(\theta_1, \varphi_1' + \Delta\varphi_1') = K(\theta_0, \varphi_0)$ really holds. The case of the second point $(\theta_1, \varphi_2' + \Delta\varphi_2')$ is similar. The error of the procedure is given by (36).

$\hat{z}$ axis. We have also proven that for the qubit key part the optimality of the $\hat{z}$ axis as the secure basis is preserved after the action of any bistochastic channel (i.e. the one represented by random Pauli rotations).

The symmetry of the ideal p-bit lead us to the heuristic scheme of estimation of the optimal axis (with respect to the Devetak-Winter secret key rate K_{DW}) which is valid for any state that has this type of symmetry of the rate under the rotation around the optimal basis. Namely given the density matrix, may be even in a numerical form, instead of searching over all sphere Alice may perform the analysis of the key over a ring around some chosen axis $\hat{z}'$ on the sphere and guess the optimal measurement axis only on the data based on this ring.

The method generally has a ,,dualistic" character with respect to the channel action. If the Alice subsystem as the direction of the optimal axis unperturbed, than the results are good if the $\hat{z}'$ is chosen to be far form the (unknown) optimal one $\hat{z}$ while if there is a perturbation of the optimal direction $\hat{z}$ (in a sense of the shrinking of that direction on a Bloch sphere) then the closer is the chosen axis to the original one the result is better. Basing on the polynomial approximation of the key function on the chosen ring there is also the possibility of the derivation of the error bar of the procedure. The analysis of examples shows that the error bar in general bounds the actual value of the error made in the procedure.

We believe that the present method may be especially useful when the large sample of data are provided and quick estimation of optimal Alice measurement is needed.

Acknowledgments. We thank Ewa and Jędrzej Tuziemscy for help in preparation of Figiures. This work was supported by 7th Framework Programme Future and Emerging Technologies project Q-ESSENCE.

[1] R. Horodecki, P. Horodecki, M. Horodecki and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009)
[2] C. H. Bennett and G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing IEEE Computer Society, New York, 1984, pp. 175179.
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. H. Bennett, G. Brassard, and N. D. Mermin, 1992, Phys. Rev. Lett. **68**, 557 (1992).
[5] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[6] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[7] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[8] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. 94, 160502 (2005).
[9] K. Dobek, M. Karpinski, R. Demkowicz-Dobrzanski, K. Banaszek, P. Horodecki, Phys. Rev. Lett. 106, 030501 (2011).
[10] K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim IEEE Trans. Inf. Theory 55, 1898 (2009).
[11] K. Dobek, M. Karpinski, R. Demkowicz-Dobrzanski, K. Banaszek, P. Horodecki Phys. Rev. Lett. 106, 030501 (2011).
[12] T. Rowland *Spherical Distance*. MathWorld–A Wolfram Web Resource, created by Eric W. Weisstein. http://mathworld.wolfram.com/SphericalDistance.html
[13] K. Horodecki, . Pankowski, M. Horodecki, P. Horodecki IEEE Trans. Inf. Theory 54, 2621 (2008).
[14] M. B. Ruskai, S. Szarek, E. Werner Lin. Alg. Appl. 347, 159 (2002).

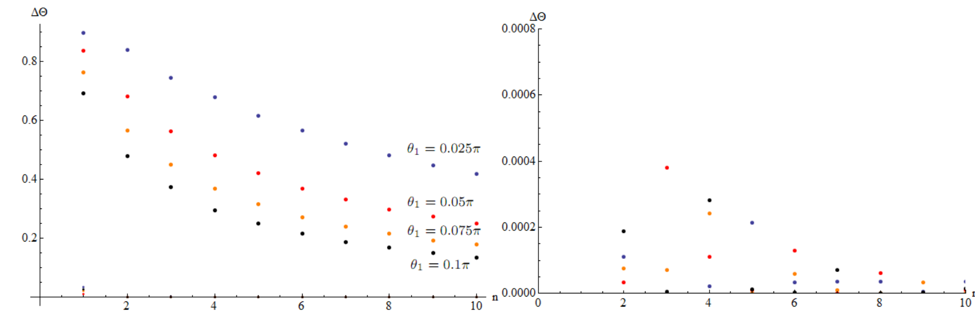

FIG. 3: The estimated error of the procedure (using formula (36)) - left plot, and the error of the procedure (absolute value of the difference between rotation angle and the angle calculated by the procedure $\Delta\theta = |\theta - \theta_{M'}|$) -right plot vs. the number of points r=10n (n=1 denotes that 10 points were used) for the rotated ρ_{SWAP} state. Rotation angle $\theta = \frac{\pi}{3}$

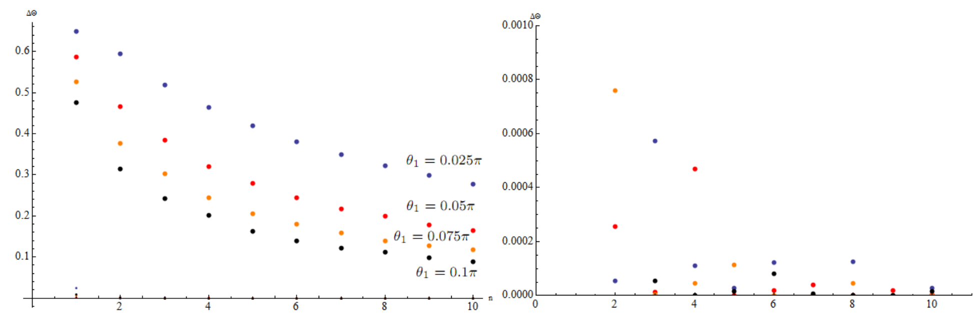

FIG. 4: The estimated error of the procedure (using formula (36)) - left plot and, the error of the procedure (absolute value of the difference between rotation angle and the angle calculated by the procedure $\Delta\theta = |\theta - \theta_{M'}|$) -right plot vs. the number of points r=10n (n=1 denotes that 10 points were used) for the state $\rho_{S\tilde{W}AP} = \Lambda_A \otimes I_{BA'B'}$, where $\Lambda(\rho) = p\frac{I}{2} + (1-p)\rho$. Rotation angle $\theta = \frac{\pi}{4}$, p=0.1.

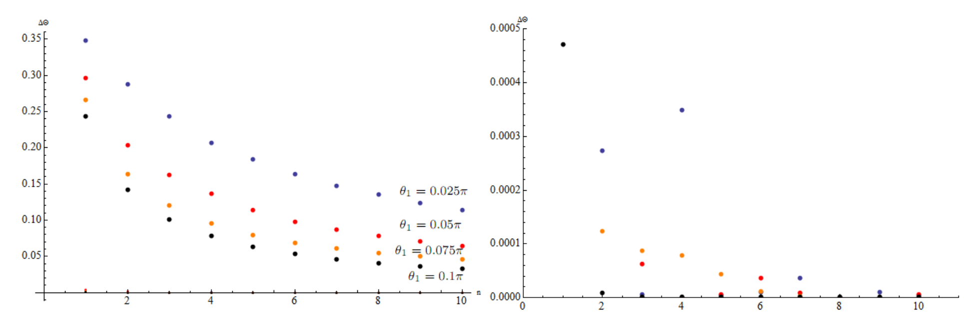

FIG. 5: The estimated error of the procedure (using formula (36)) - left plot and the error of the procedure (absolute value of the difference between rotation angle and the angle calculated by the procedure $\Delta\theta = |\theta - \theta_{M'}|$) -right plot vs. the number of points r=10n (n=1 denotes that 10 points were used) for the state $\rho_{S\tilde{W}AP} = \Lambda_A \otimes I_{BA'B'}$, where $\Lambda(\rho) = p\rho + (1-p)\sigma_z\rho\sigma_z$. Rotation angle $\theta = \frac{\pi}{7}$, p=0.3.

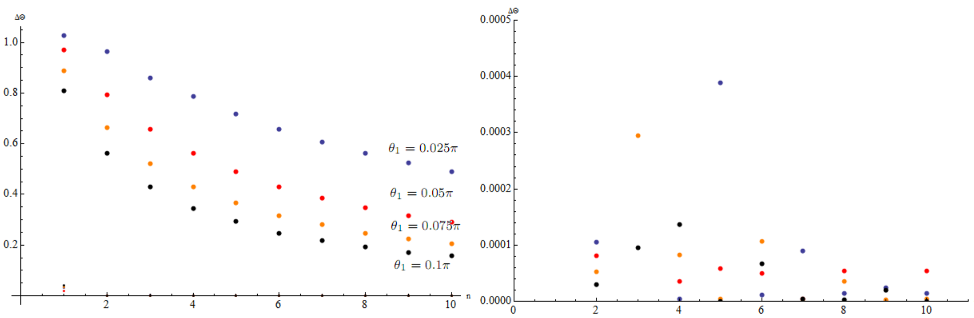

FIG. 6: The estimated error of the procedure (using formula (36)) - left plot and the error of the procedure (absolute value of the difference between rotation angle and the angle calculated by the procedure $\Delta\theta = |\theta - \theta_{M'}|$) -right plot vs. the number of points r=10n (n=1 denotes that 10 points were used) for the state $\rho_{priv} = p\rho_{SWAP} + (1-p)\rho_{MSWAP}$. Rotation angle $\theta = \frac{\pi}{8}$, p=0.4.

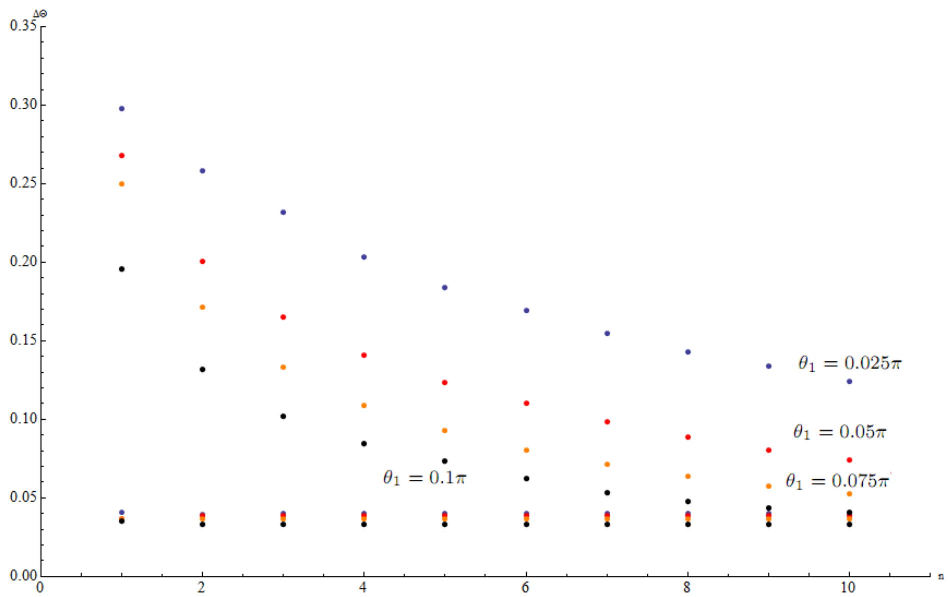

FIG. 7: The estimated error of the procedure (using formula (36)) and the error of the procedure (absolute value of the difference between rotation angle and the angle calculated by the procedure $\Delta\theta = |\theta - \theta_{M'}|$) vs. the number of points r=10n (n=1 denotes that 10 points were used) for the state $\rho_{priv} = (\Lambda_A \otimes 1_{BA'B'})\rho_{SWAP}$, $\Lambda_A(\rho) = K_1^\dagger \rho K_1 + K_2^\dagger \rho K_2$ where K_i are given by (45). Rotation angle $\theta = \frac{\pi}{8}$, u=0.1 π, v=0.05 π.